Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

SUBSTITUTION GROUPS WHOSE CYCLES OF THE SAME ORDER CONTAIN A GIVEN NUMBER OF LETTERS.

By G. A. Miller.

Let G be any transitive or intransitive substitution group, and let $a_1 a_2 \cdots a_k$ be any one of the cycles found in one or more of the substitutions of G. If this cycle and all of its conjugates under G are counted once for every substitution of G in which they appear, then the total number of letters in all of these cycles is exactly the order of G, since such a cycle is transformed into itself only by its powers by means of substitutions restricted to its own letters.* Hence the total number of letters in all the cycles of order k contained in G may be found as follows: Select a set of cycles of order k composed of all the different cycles of this order found in G. Let λ be the number of complete sets of conjugates under G contained in this set. The total number of letters in all the cycles of order k found in G is then λg, g being the order of G.

In particular, the holomorph of the cyclic group of order p, p being any prime number, contains $p - 1$ cycles of order p. Since these cycles form a single set of conjugates under this holomorph $\lambda = 1$ in this case, and hence the order of this holomorph is $p(p - 1)$, as is also otherwise evident. As another very elementary illustration it may be noted that every intransitive group of order p^m which has only transitive constituents of degree p involves only invariant cycles of order p. The number of the distinct cycles is $p - 1$ times n/p, n being the degree of the group. Hence $\lambda = n(p - 1)/p$ in this case and the total number of letters in all the substitutions of G is $n(p - 1)p^{m-1}$ as is also evident from the fact that the average number of letters in all the substitutions of an intransitive group of degree n which has k transitive constituents is $n - k$.

A necessary and sufficient condition that a group G of degree n which has k systems of intransitivity has the property that the total number of letters in all of its cycles of the same order is exactly g for every cycle which appears in these substitutions is that G contains cycles of each of the orders $2, 3, \cdots, n - k + 1$. This is clearly impossible when G is intransitive since the degree of each of these transitive constituents would be less than $n - k + 1$. Moreover, it is clear that the symmetric group of degree n involves cycles of each of the orders $2, 3, \cdots, n$, and hence this group has the property that the total number of letters in all the cycles of the same order is $n!$ for every cycle which appears in the group. It is easy to verify that the well-known triply transitive group of degree 6 and of order 120 has the same property.

---

* E. Netto, *Journal für die reine und angewandte Mathematik*, Vol. 103 (1888), p. 323.

To prove that this is the only non-symmetric group which has this property it may first be noted that if the degree of such a group would exceed 7 the group would involve a cycle of prime order p, where p satisfies the condition $n/2 < p \leqq n - 3$, according to a well-known theorem due to Tshebychef. Hence such a group must be primitive, and it cannot involve a cyclical substitution of order p without being either alternating or symmetric.* As the group could not be alternating since in the alternating group of degree n there cannot be cycles of both the orders n and $n - 1$, it must be symmetric.

It remains therefore only to prove that there is no transitive group of degree n less than 8, besides the triply transitive group of degree 6 to which we have already referred, which has the property that its substitutions involve cycles of each of the orders $2, 3, \cdots, n$. As these groups are well known this proof may be regarded as obvious, since it implies at most an examination of a few lists of substitution groups of low degrees.

To the many interesting known properties of the triply transitive group of degree 6, which was considered at length by A. L. Cauchy in volume 22 (1846) of the *Comptes Rendus*, and had been studied earlier by C. Hermite, we have here added one which all symmetric groups possess but which no other non-symmetric group possesses. This property therefore belongs to this group both when it is represented on 5 letters and when it is represented on 6 letters. In all other cases the symmetric group of degree n loses this property when it is represented on more than n letters.

The alternating group of degree n involves cycles of each of the orders $2, 3, \cdots, n$ except of order n, when n is even, or of order $n - 1$, when n is odd. Hence it results directly that the total number of letters in all the cycles of the same order contained in the alternating group is equal to the order of the group with the exception that this total is equal to twice the order of the group in the case of the largest cycle found in such a group. This follows directly from the fact that these largest cycles constitute two complete sets of conjugates under the alternating group. A necessary and sufficient condition that the holomorph of a cyclic group, written as a regular group, is composed of positive substitutions is that the orders of all the Sylow subgroups of this cyclic group are even powers of odd prime numbers.* This is evidently also a necessary and sufficient condition that all the generators of a cyclic group appear in one of the two complete sets of conjugates noted above.

---

* G. A. Miller, *Bulletin of the American Mathematical Society*, Vol. 4 (1898), p. 141.

* This fundamental theorem relating to the holomorph of a cyclic group is not found in my article on this subject, *Transactions of the American Mathematical Society*, Vol. 4 (1903), p. 153.

Besides the alternating groups there are various others which have the property that the total number of letters in all the cycles of the same order is equal to the order of the group with the exception that for one such order this number is twice the order of the group. If such a group is transitive it must involve cycles of each of the orders $2, 3, \cdots, n$ except for one such order. This condition is evidently sufficient as well as necessary. It is easily seen that the degree of such a transitive group could not exceed 15 since there are at least two distinct prime numbers which satisfy the condition $n/2 < p \leqq n - 3$ whenever n is a positive integer greater than 15. This fact can easily be verified by means of tables of primes extending to one million, and for larger values of n it results directly from known formulas. Cf. E. Landau, *Primzahlen*, Vol. 1 (1909), p. 91. In fact, from such formulas it results also that at least two such primes always exist when n exceeds a much smaller number than one million.

From the existence of at least two such primes it results directly, just as in the case of symmetric groups, that if the degree of a transitive group exceeds 15 it cannot have cycles of each of the orders $2, 3, \cdots, n$, except one, without being alternating. It is easy to verify that no non-alternating group whose degree exceeds 8 satisfies these conditions and that the group of isomorphisms of the simple group of order 168 is the only transitive group of degree 8 which is not alternating but satisfies the conditions in question. In this group of order 336, just as in the alternating groups, the number of letters in all of the cycles of the same order, except the largest one, is equal to the order of the group, while the number of letters in the cycles of order 8 is equal to 672.

There is no transitive group of degree 7 which satisfies the conditions in question but there are two such groups of degree 6, viz., the largest groups which contain 2 or 3 systems of imprimitivity. These groups are of orders 72 and 48 respectively, and the number of letters in all their cycles of lowest order is twice the order of the group while the number of letters in all of their cycles of each other order is equal to the order of the group. On 5 letters there is clearly only one such non-alternating transitive group, viz., the group of order 20, while on 4 letters the cyclic group and the octic group constitute the only instances. In the cyclic group and the group of order 20 the number of letters in the cycles of order four is equal to twice the order of the group while in the octic group this is the case as regards the cycles of lowest order.

Hence there are just six transitive groups which are non-alternating but have the property that the total number of letters in all the cycles of each order save one is the order of the group while for this one the total number of letters is twice the order of the group. Three of these have in common with all the alternating groups the property that the cycles in which the largest number of letters appear are also the largest cycles, while in the other three the largest number of letters appear in the smallest cycles.

If in a constituent of an intransitive group the total number of letters found in all of its cycles of the same order is k times the order of this constituent, then the total number of letters found in these cycles for all the substitutions of the entire group is also equal to k times the order of this group. In particular, if each of k constituents of an intransitive group contains a cycle of the same order, then the total number of letters in all the cycles of this order contained in the group is at least k times the order of the group. Hence it results that if an intransitive group has the property that the total number of letters found in its cycles of the same order, except one, is equal to the order of the group and for this one it is equal to twice this order, then no more than two of its transitive constituents can involve cycles of the same order. If two such constituents involve cycles of the same order, the total number of letters in all the cycles of the same order found in these constituents must be the order of the constituent.

It is evident that the intransitive groups which have for one constituent the regular group of order 2 and for the other any symmetric group, or the triply transitive group of degree 6, satisfy the condition that the total number of letters found in their cycles of order 2 is twice the order of the group while the total number of letters in all of the other cycles of the same order is equal to the order of the group. Moreover, these are the only intransitive groups in which at least two transitive constituents have cycles of the same order and which, moreover, satisfy the condition that the total number of letters found in the cycles of one order is twice the order of the group while the total number of letters found in all the cycles of every other order is equal to the order of the group. If no two transitive constituents have cycles of the same order, the orders of these constituents must be relatively prime.

As the orders of all the transitive groups which have the property that either the total number of letters in the cycles of the same order is equal to the order of the group for every order of such a cycle, or this is true of all cycles except those of one order in which the total number of letters involved is twice the order of the group, are even with the exception of the alternating group of degree 3, it remains therefore only to consider the intransitive groups having for one constituent this alternating group. The other constituent is evidently the symmetric group of order 2, and hence the intransitive cyclic group of degree 5 and order 6 is the only intransitive group which has the property that the total number of letters in every cycle of the same order except one is equal to the order of the group and that the number of letters in the cycles of this particular order is equal to twice the order of the group while the orders of the transitive constituents are relatively prime.

If no two of the complete set of conjugates of a given cycle of a transitive group have a common letter, then these conjugates constitute a substitution which is invariant under the transitive group. Moreover, if a substitution is invariant under a transitive group, its subgroup which is composed of all its substitutions omitting one letter must omit more than one letter, and hence the group must *involve* a cycle whose conjugates under the group have no common letter. That is, *a necessary and sufficient condition that there is a substitution, besides the identity, which is commutative with every substitution of a transitive group is that the group involves a cycle such that no two of the conjugates of this cycle under the group have a common letter.* The total number of substitutions which are commutative with every substitution of a transitive group is therefore equal to the number of its different cycles which involve the same letter and have the property that no two of the cycles in any one of the complete sets of conjugates to which they separately belong have a common letter.

As the total number of letters found in identical cycles and all their conjugates is equal to the order of the group, it results directly that the number of cycles which are identical with a cycle having the property that no two of its conjugates involve the same letter is equal to the order of the group divided by its degree. In particular, the number of such cycles which are identical is an invariant of the substitution group. A necessary and sufficient condition that a transitive group is regular is that every one of its cycles has the property that no two of its conjugates under the group have a common letter. The $g - 1$ complete sets of conjugates of the cycles of a regular group G of order g give rise to $g - 1$ substitutions which are separately commutative with every substitution of G. The fact that these $g - 1$ substitutions together with the identity constitute a group follows directly from the facts that all the substitutions which are commutative with every substitution of G must constitute a group and that each such substitution besides the identity must be of degree g. We thus have a new proof of the fact that all the substitutions which are commutative with each substitution of a regular group of order g constitute a regular group of this order.

Since every transitive group whose order is of the form p^m, p being a prime number, involves invariant substitutions, it results that it involves cycles such that no two of their conjugates under the group involve a common letter. When the group is non-regular each such cycle must appear in more than one substitution. In fact, the number of substitutions in which it appears is always equal to the order of the group divided by its degree even when the order of the group is not a power of a prime. In particular, when the degree of a group of order p^m is p^2, $m > 2$, its only cycles which appear in more than one substitution are those which are found in its invariant subgroup of order p. That is, *in every transitive group of degree p^2 and of order p^m, $m > 2$, the total number of letters found in the conjugates of every cycle which does not appear in the invariant subgroup of order p is equal to the order of the group.*

If a transitive group of degree n is regular or of class $n - 1$, it evidently cannot involve two substitutions which contain the same cycle. It is not difficult to prove that every other transitive group contains such substitutions. To prove this theorem, let G be any transitive group of degree n which involves at least one substitution s whose degree does not exceed $n - 2$. If G is at least doubly transitive, it must involve a cycle of order 2 which does not involve any of the letters of s. The subgroup generated by s and a substitution involving this cycle will clearly have this cycle in one half of its substitutions, and as the order of this subgroup exceeds 2 it may be assumed in what follows that G is simply transitive. It will also be convenient to assume that G is a group of lowest possible degree which does not involve two substitutions containing the same cycle but involves at least one substitution whose degree does not exceed $n - 2$.

The subgroup G_1 composed of all the substitutions of G which omit a given letter is of degree $n - \alpha$. If $\alpha > 1$, it is well known that G_1 is invariant under an intransitive group which has one transitive constituent of degree α. This intransitive group evidently involves at least two substitutions containing the same cycle. Hence it may be assumed that $\alpha = 1$ and that G_1 is formed by a simple isomorphism between transitive groups of which at least one is of a class one less than its degree while the others, if any, are regular. If a transitive group of degree k and of class $k - 1$ can be represented in more than one way as a transitive group whose degree is exactly one unit larger than its class, every invariant regular subgroup must include all the subgroups which appear in the regular form when the group is represented on a smaller number of letters. This follows directly from the fact that in a transitive group of degree k and of class $k - 1$ every substitution of degree $k - 1$ is transformed into k distinct substitutions by the substitutions of the regular subgroup of order k and this subgroup of order k must be found in every invariant subgroup which involves a substitution of degree $k - 1$.

The substitution s may be supposed to be found in G_1. If the group generated by s is transformed into itself by a substitution of G which is not found in G_1, this substitution and s will clearly generate an intransitive group having a constituent whose order is less than the order of this intransitive group and therefore a cycle which appears in more than one of its substitutions. Hence it may be supposed that s is transformed under G into a substitution of G_1 with which it is not conjugate under G_1. As this substitution may be supposed to involve the same letters as s does, it results that the transforming substitution and s again generate an intransitive group involving a constituent whose order is less than the order of this intransitive group. Hence it has been proved that *a necessary and sufficient condition that a transitive group of degree n contains a complete set of distinct conjugate cycles whose total number of letters is less than the order of the group is that the class of the transitive group is less than* $n - 1$.

If a substitution group of degree n involves cycles of order n or of order $n - 1$, the total number of letters in a complete set of conjugates of such a cycle is always equal to the order of the group since such a cycle cannot appear in two different substitutions. This is a special case of the evident theorem that if a group of degree n involves a cycle of order $n - \alpha$ but no substitution on α or less than α letters, then the total number of letters in all the conjugates of this cycle must equal the order of the group. In particular, if a primitive substitution group of degree n involves a complete set of conjugate cycles of order $n - 2$ such that the total number of letters in all the cycles of the set is less than the order of the group, the group must be the symmetric group of degree n, and if an imprimitive group of degree n involves such a complete set of conjugates, n must be even and the group must involve the abelian subgroup which has for its independent generators $n/2$ transpositions.

In the preceding paragraph there appears a new definition of the symmetric group. As another such definition we give the following: The symmetric group of degree n is the transitive group of this degree in which each cycle of order 2 appears in $(n - 2)!$ substitutions. It may also be noted that if a multiply transitive group of degree n is not of class $n - 1$, then each of its cycles of order 2 must be found in more than one substitution. In fact, each such cycle can be transformed into every other such cycle since the group is at least two times transitive. Some such cycle must appear in more than one substitution, since the cycle of order 2 which involves the letter a, for instance, must involve another letter which does not appear in at least two of the substitutions of the subgroup composed of all the substitutions which omit a. Hence the theorem: *Every cycle of order 2 found in a multiply transitive group appears in more than one substitution whenever the class of this group is not one less than its degree.*

UNIVERSITY OF ILLINOIS